DOI 10.26886/2520-7474.2(28)2018.4

UDC 343.985.7

CRIMINALISTIC CLASSIFICATION OF HARMFUL SOFTWARE

O. Volkov

National Academy of Internal Affairs, Ukraine, Kiev

The essence and content of the notion of forensic classification of harmful software tools are analyzed, their characteristic forensic features and properties are determined. The stages of creation of malicious software and objects of their influence are considered. The signs were investigated, classification criteria for attributing a malicious software to one or another type were determined. The necessity of creating a single forensic classifier for malicious software is substantiated.

Key words: computer viruses, cybercrime, unauthorized access, hackers, electronic computing, computer networks.

Волков О. О. Криміналістична класифікація шкідливих програмних засобів/ Національна академія внутрішніх справ, Україна, Київ

Проаналізовано сутність та зміст поняття криміналістичної класифікації шкідливих програмних засобів, визначено їх характерні криміналістичні ознаки та властивості. Розглянуто стадії створення шкідливих програмних засобів та об'єкти їх впливу. Досліджено ознаки, визначено класифікуючі критерії віднесення шкідливого програмного засобу до того чи іншого виду. Обґрунтовано необхідність створення єдиного криміналістичного класифікатора шкідливим програмним засобам.

Ключові слова: комп'ютерні віруси, кіберзлочинність, несанкціонований доступ, хакери, електронно-обчислювальна техніка, комп'ютерні мережі.

Постановка проблеми. На теперішній час існує цілий ряд класифікацій ШПЗ з різними їх проявами, негативними наслідками, середовищем існування. Подекуди один і той же ШПЗ має властивості, що підпадають під різні види існуючих класифікацій, що на практиці значно ускладнює процес опису та документування таких злочинів.

Актуальність дослідження. Упровадження загальноєвропейських норм у протидії злочинності у тому числі і кібернетичної вимагає від правоохоронних органів чіткого дотримання прав людини, її свободи, честі, гідності. Такі цінності є визначальними та пріоритетними при побудові правової держави та трансформації до Європейського суспільства. Ефективність розслідування кіберзлочинів у першу чергу залежить від фахового рівня правоохоронців, чіткого розуміння такого явища, уміння розрізняти одні види злочинів від інших.

Відсутність єдиної криміналістичної класифікації «шкідливого програмного засобу» (далі – ШПЗ) має наслідком унеможливлення єдиного підходу до ефективної протидії такому суспільно-небезпечному явищу, пошуку та фіксації слідів такої діяльності.

Ціль статті. Дослідження та узагальнення криміналістичної класифікації ШПЗ які створені, використовується та розповсюджуються для несанкціонованого втручання в роботу ЕОТ, комп'ютерів, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку (далі – електронно-обчислювальна техніка, ЕОТ), з метою сприяння ефективній протидії кіберзлочинності.

Різним аспектам криміналістичної класифікації ШПЗ, у тому числі їх характеристики, зовнішнім проявам, механізму впливу на інформацію, що зберігається в ЕОТ, присвячували свої роботи В. Г. Хахановський, А. С. Білоусов, П. Д. Біленчук, О. А. Федотов, К. С. Архіпов, Р. С. Бєлкін, І. С. Биховський, В. В. Крилов, Б. В. Романюк,

Л. М. Соловйов, Т. Л. Тропіна, В. С. Цимбалюк та інші вчені. Однак питання криміналістичної класифікації у цій сфері досліджено не повною мірою.

Світова цивілізація вже давно вступила в еру інформації. З кожним днем активніше розвиваються сучасні інформаційні технології і в Україні [1, 6]. Комп'ютерні технології використовуються практично в усіх сферах та галузях зв'язку, енергетики, транспорту, державними органами та багатьма іншими установами [2, 77]. Як зазначають П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та інші поширення інформаційних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінки [3, 57].

Кількість злочинів, вчинених у кіберпросторі, росте пропорційно кількості користувачів комп'ютерних мереж, і, по оцінках Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет є найшвидшими на планеті [4, 36].

Характерною особливістю кіберзлочинів, що відрізняє їх від всіх інших кримінально-караних діянь, є те, що вони мають високий рівень латентності. Так, кількість вражень ШПЗ і хакерських атак в Україні значно зросла з 10 млн. у 2016 до 100 млн. у 2017 році [5].

Однак органами досудового розслідування Національної поліції України в 2017 році обліковано та розпочато досудове розслідування лише в 2514 кримінальних правопорушеннях у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. З указаної кількості лише 32 кримінальних правопорушень відповідальність за які передбачено ст. 361-1 КК України (Створення з метою використання, розповсюдження або збут шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут). Водночас з указаної кількості

повідомлено про підозру лише у кожному четвертому кримінальному правопорушенні (7) стільки ж проваджень направлено до суду [6].

Причиною такої суперечливої динаміки, як зазначають деякі дослідники є не фактичний стан злочинності, так як загальна тенденція – це зростання числа кіберзлочинів, а зміни в правової політиці держави, відомств, органів, що займаються виявленням, обліком, розслідуванням і розкриттям даної категорії злочинів [7, с. 31]. Інші вчені стверджують, що це пов’язано з різними методиками обчислення кількості вказаних злочинів правоохоронними органами [8, с. 126].

Кіберзлочинці вміло маскують свої атаки, використовують для цього недосконаліть програмних засобів, але при цьому постійно вдосконалюють свою тактику, проводячи випробування створених ШПЗ, що призводить до блокування засобів контролю і управління.

Зловмисники застосовують ШПЗ для шифрування інформації в ЕОТ, використовують легальні інтернет-сервіси, для приховування своєї діяльності, подолання традиційних систем захисту.

Для ефективної протидії злочинності пов’язаної із застосуванням ШПЗ виникла необхідність в їх уніфікованій класифікації. Першими ініціативу у свої руки взяли комерційні структури.

Разом зі створенням перших антивірусних програм у фахівців чий бізнес був пов’язаний із протидією ШПЗ виникла необхідність класифікації виявлених ними об’єктів. У той час шкідливих програм було небагато, проте, необхідно було придумати спеціальні назви, щоб відрізняти їх один від одного. Творці перших антивірусних програм застосовували в практиці найпростішу типологію, яка складалася з власного імені вірусу і розміру виявленого файлу. Однак іноді виникала плутанина через те, що один і той же шкідливий програмний засіб носив різні імена в різних антивірусних системах.

Так, ім'я кожному ШПЗ надавалося антивірусною компанією відповідно до її власної класифікації, прийнятої в конкретній компанії, зрозуміло, що така класифікація була різною. Так, наприклад шкідливий програмний засіб який називається Worm.Win32.Nuf в іншій компанії називався Net-Worm.Win32.Mytob.c. проте це один і той же ШПЗ.

Іншими антивірусними компаніями назви шкідливих програмних засобів надавалися за певними зовнішніми ознаками, наприклад, за місцем виявлення шкідливого програмного засобу (Jerusalem); за змістом або виведення текстового повідомлення (I Love You); методу подачі користувачеві (AnnaKournikova); від демонструючого візуального ефекту (Black Friday).

На початку дев’яностих років минулого століття було здійснено ряд спроб уніфікувати процес класифікації шкідливих програмних засобів. Першими в цьому напрямку були учасники альянсу антивірусних фахівців (англ. Computer AntiVirus Researcher's Organization, CARO [9]). В процесі діяльності альянсом був складений документ під назвою «CARO malware naming scheme», принципи якого стали еталоном для всієї антивірусної індустрії.

З часом ряд факторів привів до того, що ці принципи стало неможливо застосовувати на практиці. Одним з них став швидкий і стрімкий розвиток ШПЗ, упровадження в масове користування нових операційних систем, технічних пристроїв, збільшення кількості антивірусних програмних засобів. Але ще більш значущою причиною відмови фахівців від використання зазначеної схеми стало те, що антивірусні корпорації стали пропонувати свої технології обробки інформації і виявлення ШПЗ.

У свою чергу це призвело до того, що результати роботи різних програм стало неможливо порівняти між собою і яким-небудь чином

стандартизувати. Так чи інакше, сьогодні робляться спроби ще раз повернутися до цієї проблеми і все ж вивести єдину схему типології виявляемих ШПЗ. Але більшою мірою такі спроби залишаються безрезультатними. Серед останніх подій в цьому напрямку значиться створення організації CME (Common Malware Enumeration)[10], мета якої присвоєння унікального ідентифікатора однаковим об'єктам, виявляємих антивірусними програмами.

Серед існуючих класифікацій ШПЗ не всі мають значення для криміналістичних досліджень, тому що створення таких класифікацій частіше було підпорядковано прикладним завданням виявлення та знищення вірусів. Для криміналістики цікавими є відомості, які характеризують наслідки дій ШПЗ та їх найбільш явні та характерні прояви.

Зазначимо, що неточність під час опису ШПЗ, процесу його створення та механізму його несанкціонованого застосування може суттєво відобразитися на документуванні такої протиправної діяльності.

Так, розглядаючи діяльність по створенню шкідливих програмних засобів необхідно звернути увагу на те, що всім ШПЗ при їх створенні притаманні наступні стадії їх розроблення, а саме:

- постановку завдання, визначення середовища існування і мети застосування;

- вибір засобів і мов програмування ШПЗ;

- написання безпосереднього тексту (лістингу) ШПЗ;

- відладка ШПЗ, перевірка відповідності їх функцій з поставленими завданнями);

- запуск і безпосередню дію ШПЗ (випуск, надання інформації).

Під час проведення досудового розслідування та документування такої протиправної діяльності дії щодо постановки завдання,

визначення середовища існування і мети ШПЗ, вибору засобів і мов програмування можуть знайти відображення в показах свідків, чорнових роздруківках документах лістингів, листуванні, які вказують на проведення певної роботи та зацікавленості особи в даній проблематиці.

Документування написання безпосереднього тексту програми (програмування), її відладки можуть відображатися у чернетках на традиційних та магнітних носіях інформації, в свідченнях осіб які спостерігали за процесом відладки або його результатами.

Діяльність щодо запуску і безпосередньої роботи ШПЗ можуть бути зафіксовані як у свідченнях очевидців, так і під час прояву шкідливих суспільно небезпечних наслідків. Кожна з цих елементарних дій за умови існування наміру створення ШПЗ та існуванні об’єктивно виражених слідів його існування можуть бути предметом криміналістичного дослідження і кримінально-правової оцінки під час доказування на досудовому слідстві.

Перед розглядом криміналістичної класифікації ШПЗ необхідно розглянути що саме може бути об’єктом впливу ШПЗ.

Так, усі без виключення ШПЗ можуть вражати:

1. *Виконувані файли, тобто файли з розширеннями імен .com і .exe, а також оверлейні файли, що завантажуються при виконанні інших програм*.

Такі ШПЗ, що вражають файли, називаються файловими. ШПЗ в уражених файлах починає свою роботу під час запуску тієї програми, в якій він знаходиться. Найбільш небезпечні ті ШПЗ, які після свого запуску залишаються в пам'яті резидентно - вони можуть вражати файли і виконувати шкідливі дії до наступного перезавантаження комп'ютера. А якщо вони вразять будь-який програмний засіб з

автозапуску комп'ютера, то і при перезавантаженні з жорсткого диска ШПЗ знову почне свою роботу.

2. *Завантажувач операційної системи і головний завантажувальний запис жорсткого диска*.

ШПЗ, що вражає ці області, називаються завантажувальними. Такий вірус починає свою роботу при початковому завантаженні комп'ютера і стає резидентним, тобто постійно знаходиться в пам'яті комп'ютера. Механізм поширення завантажувальних ШПЗ полягає в ураженні завантажувальних записів шляхом зчитування комп'ютером змінних носіїв інформації (флешнакопичувачі, оптичні диски).

Часто такі ШПЗ складаються з двох частин, оскільки завантажувальний запис має невеликі розміри і в них важко розмістити повністю тіло ШПЗ. Частина ШПЗ розташовується в іншій ділянці диска, наприклад, в кінці кореневого каталогу диска або в кластері в області даних диска. Зазвичай такий кластер оголошується дефектним, щоб виключити затирання ШПЗ під час запису даних на диск.

3. *Файли документів, інформаційні файли баз даних, таблиці табличних процесорів і інші аналогічні файли* можуть бути заражені макровірусами. Макро-віруси використовують можливість вставки в формат багатьох документів макрокоманд.

У подальшому, після реалізації свого злочинного умислу по створенню ШПЗ всі їх різновиди та модифікації можна класифікувати за наступними категоріями:

По середовищу існування ШПЗ розділяються на *файлові, завантажувальні, файлово-завантажувальні, макровіруси* та *мережеві*.

Файлові. До появи Інтернету саме «віруси» були найпоширенішими. На сьогоднішній день відомі шкідливі програми, що вражають всі типи виконуваних об’єктів будь-якої операційної системи

(для Windows небезпеці наражаються виконавчі файли (.exe, .com), командні файли (.bat), драйвера (.sys), динамічні бібліотеки (.dll) та допоміжні програмні засоби.

Ураження відбувається наступним чином. ШПЗ записує свій код в файл-жертву. Крім того, заражений файл спеціальним чином змінюється. В результаті при зверненні до нього операційної системи (запуск користувачем, виклик з іншої програми і т.п.) управління передається в першу чергу коду цього ШПЗ, який може виконати будь-які дії, задані йому творцем. Після виконання своїх дій ШПЗ передає управління програмі, яка виконується нормальним чином. Якщо на комп'ютері користувача не встановлено спеціальне програмне забезпечення, з яким це ЩПЗ запрограмовано взаємодіяти, він може довго не здогадуватися про знаходження на його комп’ютері ШПЗ.

Завантажувальні. Це ШПЗ вражає завантажувальні сектори жорстких дисків (Boot-сектор), або сектор що містить системний завантажувач жорсткого диска компютера (Master Boot Record). У такому випадку ШПЗ додає свій код до однієї зі спеціальних програм, які починають виконуватися після включення комп'ютера до завантаження операційної системи. В завдання цього спеціального програмного забезпечення якраз і входять підготовка і запуск операційної системи. Таким чином, ШПЗ отримує управління і може виконати певні дії, наприклад записати себе в оперативну пам'ять. І тільки після цього буде завантажуватися операційна система. За таких умов ШПЗ на той момент вже буде знаходитися в пам’яті і зможе контролювати роботу як операційної системи, так і антивірусних засобів.

Файлово-завантажувальні. ШПЗ, що вражають як файли, так і завантажувальні сектори. Таке ШПЗ, як правило, має складний

алгоритм роботи, часто використовує нестандартні методи несанкціонованого проникнення в систему і їх важче виявити.

Макровіруси. Це різновид ШПЗ, який являє собою програми, які розроблені на мовах, вбудованих в різні програмні системи. Найчастіше жертвами стають файли, створені різними компонентами Microsoft Office (Word, Excel). Вбудований в ці програмні продукти Visual Basic найкраще підходить для створення макровірусів.

Принцип їх дії простий. Такий ШПЗ записує себе в DOT-файл, в якому містяться всі глобальні макроси, частина з яких він підміняє собою. Після цього всі файли, збережені в цій програмі, будуть містити макровіруси. При цьому він може виконувати безліч різних деструктивних дій.

Мережеві віруси. Головною особливістю цих ШПЗ є самопоширення через мережу, можливість працювати з різними мережевими протоколами. Тобто, вони можуть різними шляхами записувати свій код на віддаленому комп'ютері. Найбільшого поширення в наш час отримали інтернет-хробаки. Такі ШПЗ найчастіше використовують для своєї роботи електронну пошту, «прикріпившись» до листа. При цьому на комп'ютері одержувача такої пошти вони або автоматично виконуються, або різними способами спонукають користувача до свого запуску.

По зовнішньому вигляду поділяються на: *звичайні, приховані, поліморфні*.

Звичайні - програмний вигляд ШПЗ, його оболонку видно у файловій системі та на жорсткому диску.

Приховані - програмний вигляд ШПЗ, без спеціального програмного засобу не відображається в файловій системі та на жорсткому диску.

За результатами деструктивної діяльності: *нешкідливі, безпечні, небезпечні, особливо небезпечні*.

Нешкідливі. Не виконують шкідливі дії. Не впливають на роботу комп'ютера, але зменшують обсяг вільної оперативної пам'яті і пам'яті на дисках, дії таких програмних засобів проявляються в графічних або звукових ефектах, або шляхом самокопіювання.

Безпечні. Не заважають роботі комп'ютерів, але зменшують обсяги вільної пам'яті і місце на жорстких дисках, дії таких ШПЗ проявляються в графічних чи звукових ефектах.

Небезпечні. Виконують шкідливі дії, що призводить до різних деструктивних наслідків До них відносяться ШПЗ, які можуть привести до збоїв в роботі операційної системи або деяких програм.

Особливо небезпечні. Ці ШПЗ можуть знищити визначену або всю інформацію, що знаходяться на жорсткому диску, змінити системну інформацію, вивести з ладу операційну систему, окрему комп'ютерну програму.

Файли, які в звичному розумінні не являються ШПЗ, але в більшості випадків є небажаним їх знаходження на комп'ютері користувача:

- **жартівливе**, що виконує будь-які речі, що турбують користувача;

- **adware** програмне забезпечення, що показує рекламу, або при користуванні браузером відкриває окремі вікна, як правило це ігрові азартні сервіси, легальна реклама яких неможлива;

- **spyware** програмне забезпечення, яке займається масовим збиранням на перший погляд малоцінної інформації, наприклад, конфігурації комп'ютера, каталогів диска, активності користувача для всілякого роду рейтингових агентств, подальшої подачі такому користувачу цілеспрямованої реклами.

Документи з ураженим шкідливим програмним забезпеченням вмістом, дестабілізуюче програмне забезпечення, наприклад, текстовий документ з включеним у нього макрокоманд, ціль якого уповільнити роботу комп'ютера, архів розміром менше мегабайта може містити в собі гігабайти даних і при розпакуванні їх надовго вивести з нормальної роботи архіватор.

Програмне забезпечення віддаленого адміністрування може застосовуватися як для того щоб дистанційно допомогти користувачу вирішите проблемне питання на його комп'ютері так і для протиправних цілей.

Руткіт потрібен для того, щоб приховувати інший ШПЗ від сторонніх осіб, систем захисту та користувача.

Інколи ШПЗ для свого функціонування встановлюють додаткові утиліти, програмні маршрутизатори, відкриті бібліотеки команд перехоплення натискання клавіатури. Таке програмне забезпечення «шкідливим» не являється, але із-за того що вони використовуються ШПЗ антивірусними засобами детектується як «шкідливе».

За способом ураження можна поділити на *резидентні* та *нерезидентні*.

Резидентні. Найчастіше такі ШПЗ є однією з найнебезпечніших файлових і завантажувальних різновидів.

Резидентний вірус при враженні (інфікуванні) комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення операційної системи до об'єктів зараження (файлів, завантажувальних секторів дисків і т.п.) і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до вимикання або перезавантаження комп'ютера.

Нерезидентні. ШПЗ, що не вражають оперативну пам'ять комп'ютера і є активними лише обмежений час.

За особливостями алгоритму дії ШПЗ важко класифікувати через велике їх розмаїття. Однак з їх кількості можна поділити на наступні *великі групи*:

Найпростіші. Такі ШПЗ змінюють вміст файлів і секторів диска, можуть бути досить легко виявлені і нейтралізовані. Можна відзначити віруси-реплікатори, що називаються хробаками, які поширюються по комп'ютерних мережах, встановлюють адреси мережевих комп'ютерів та поширюють за цими адресами свої копії.

Комп'ютерний вірус. Найбільш поширений різновид ШПЗ, що самопоширюється в межах простору жорсткого диску комп'ютера, комп'ютерних мережах, а також через змінні носії інформації (флеш-накопичувачі, оптичні диски). Комп'ютерні віруси, в свою чергу, діляться за наступними типами:

- компаньйон-віруси (companion). Алгоритм роботи цих вірусів полягає в тому, що вони створюють для EXE-файлів файли-супутники, що мають те ж саме ім'я, але з розширенням COM. При запуску такого файлу DOS першим виявить і виконає COM-файл, тобто вірус, який потім запустить і EXE-файл;

- **паразитичні**. Всі віруси, які при поширенні своїх копій обов'язково змінюють вміст дискових секторів або файлів.

- **стелс-віруси** (stealth - невидимка). Це віруси, які вміють приховувати свою присутність в системі, що ускладнює їх виявлення. Стелс-віруси використовують різні способи забезпечення «прихованості».

Найбільш поширений наступний їх варіант. Вірус складається з двох частин. Одна з них резидентна і постійно знаходиться в пам'яті комп'ютера. Якщо антивірусна програма звертається до враженого файлу, то «резидент» перехоплює це звернення і видаляє з файлу код вірусу. Таким чином, перевіряємий сегмент виявляється «чистим». Але

після того як воно завершує свою роботу, «резидент» знову його вражає.

Поліморфні (або примари, polymorphic). Особливістю цих ШПЗ є вміння змінювати власний код. Така конструкція спеціально пристосована для переховування від антивірусних програм, у своїй конструктивній частині не містять жодної постійної ділянки коду. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

Поліморфні ШПЗ бувають двох типів. Перші просто шифрують власне «тіло» з непостійним ключем і випадковим набором команд дешифратора. Друга група складніша. ШПЗ, що відносяться до неї, можуть переписувати свій код, тобто, по суті, вони самі є програмістами.

Троянський кінь. ШПЗ який містить у собі деякі деструктивні функції, яка активуються при настанні деяких умов для їх активації. Зазвичай такі ШПЗ маскуються під які-небудь прикладні корисні утиліти, ігрові або розважальні програми від чого і пішла їх назва. Особливістю такого ЩПЗ є те, що в нього немає самодостатнього механізму самопоширення, що в першу чергу пов’язано із завданнями які перед ним ставляться розробником.

Мережевий черв’як або хробак (worm). Називають ШПЗ, що не пов’язують свої копії з якимись файлами. Вони створюють свої копії на жорстких дисках і в підкаталогах дисків не змінюючи інших файлів. Такі віруси іноді створюють робочі файли на дисках системи, але можуть взагалі не звертатися до ресурсів комп'ютера (за винятком оперативної пам'яті). Наприклад, XMasTree, Morpica (Internet Worm).

Поширюються по глобальних мережах, вражаючи як окремі програми так і цілі комп’ютерні системи. Це найнебезпечніший вид

вірусів, так як об'єктами враження в цьому випадку стають інформаційні системи глобального масштабу.

Логічна бомба. Різновид ШПЗ який знаходячись в операційній системі активує свої деструктивні функції при певних умовах та є складовою програмного коду корисного програмного забезпечення.

Руткіти. ШПЗ що представляють собою більш високотехнологічний варіант троянських коней. Однак на їх відміну руткіти використовують для маскування більш просунуті методи, проникаючи глибоко в операційну систему комп'ютера. Словом «руткіт» визначається набір різних програмних кодів, що дозволяє зловмисникові повертатися у зламану систему поза увагою системного адміністратора, а системи захисту ЕОТ не могли бачити таке несанкціоноване проникнення.

Бекдор (backdoor, back door - чорний хід). ШПЗ, які встановлює правопорушник після отримання несанкціонованого доступу до комп'ютера з метою повторного отримання доступу до системи.

Основне призначення Backdoor є несанкціоноване управління комп'ютером. Як правило, використовуючи Backdoor правопорушник може віддалено виконувати будь-що на комп'ютері жертви (доступ до реєстру операційної системи, змінювати паролі, проводити системні операції, перезавантажувати комп'ютер).

Експлойт. Теоретично нешкідливий набір даних (наприклад, графічний файл або мережевий пакет), що некоректно сприймається програмою, що обробляє такі дані. В цьому випадку шкоди завдає не сам файл, а неадекватна поведінка програмного забезпечення з помилкою. Також експлойтами називають програмні засоби створені для генерації подібних наборів програмних кодів з «пошкодженними» даними.

Кейлоггер (keylogger). ШПЗ, основним призначенням якого є прихований моніторинг натискань клавіш і ведення журналу цих натискань.

По шкідливим наслідкам - перешкоджання роботи комп'ютера починаючи від відкриття-закриття DVD-ROM і закінчуючи знищенням інформації та поламками технічних засобів. Наприклад, Win32.CIH. характерний саме поломками технічних засобів комп'ютерної техніки.

Викрадення інформації що знаходиться на комп'ютері користувача, (особистих даних, номера кредитних карток, інтернет-гаманців, а також грошей що там містяться). Для крадіжки може використовуватися сканування жорсткого диску, реєстрування натискання клавіши на клавіатурі (Keylogger), перенаправлення користувача на підроблені сайти (Фішинг), що повністю відтворює ресурси справжнього сайту.

Крадіжка акаунтів різних сервісів (електронна пошта, інтернет-месенджери, ігрові сервери). Аккаунти застосовуються для розсилання спама, використовуються від імені власника, ігрові акаунти в мережевих іграх найчастіше викрадаються з метою подальшої перепродажу, так як в них як правило для розвитку ігрового героя вкладаються кошти, або шантажу власнику з метою отримання неправомірної вигоди за його повернення.

Блокування антивірусних сайтів, антивірусного програмного забезпечення і адміністративних функцій операційної системи з метою ускладнити нейтралізацію або знищення ШПЗ.

Шахрайство, наприклад отримання коштів за розблокування роботи або розшифрування інформації що знаходилася на комп'ютері, та було раніше заблоковано або зашифровано раніше встановленим ШПЗ (Ransomware). В більшості випадків, після отримання коштів після

здійсненні оплати інформація на комп'ютері або не розблоковується, або через деякий час блокується знову.

Вимагання, під виглядом сплати штрафу на користь правоохоронного органу за нібито відвідування заборонених інтернет-сайтів, виявлення на комп'ютері жертви недозволеного або інтимного контенту.

Саботування промислових процесів, що управляються комп'ютерами, наприклад «компютерний хробак» «Stuxnet». Встановлення (інсталяція) іншого ШПЗ.

Завантаження з мережі (downloader) будь-якої інформації без відома користувача комп'ютера, або розпакування іншого ШПЗ, що міститься всередині файлу (dropper).

Використання телефонного модему, або функцій телефону, у разі користування інтернет-месенджерами що здатні здійснювати дзвінки на телефонні номери стаціонарної системи зв'язку для здійснення дзвінків на номери з дорогими вхідними або вихідними тарифами, що тягне за собою списання коштів з рахунку або акаунта та отримання значної суми для оплати за користування засобами зв'язку.

Отримання оплати за програмне забезпечення, яке імітує роботу наприклад, антивірусного програмного забезпечення, однак не виконує своїх функцій (fraudware або scareware).

ШПЗ призначені для іншої несанкціонованої діяльності.

Отримання несанкціонованого доступу до ресурсів комп'ютера або іншим ресурсам здійснюваного через такий комп'ютер, у тому числі пряме управління комп'ютером (backdoor).

Організація на комп'ютері відкритих поштових релеїв та загальнодоступних проксі-серверів.

Уражений ШПЗ комп'ютер (в складі ботнета) може бути використаний для проведення DDoS-атак.

Збір адресів електронної пошти та поширення спаму, у тому числі в складі «ботнета».

Підвищення рейтингу в інтернет-сервісах, соціальних мережах, інтернет-голосуваннях, підвищення кількості відвідувань по рекламних «банерах».

Генерація криптовалюти різних платіжних засобів (Bitcoin, Ethereum, Litecoin, Dash, Nem).

По операційним системам для враження яких створено ШПЗ:

- для маршрутизаторів (Cisco IOS, PIX OS, LinkBuilder, MikroTik і т.п.);

- для мобільних пристроїв (Symbian OS, Palm OS, WebOS, Android, iOS, Tizen, Bada, Blackberry OS, Windows CE);

- для персональних комп'ютерів і серверів (MacOS, Windows, Solaris, GNU/Linux, FreeDOS)

Не залежно від класифікації необхідно зазначити, що всі ШПЗ мають загальні характерні їм властивості. Так, потрапивши в середовище свого існування ШПЗ проходить наступні технічно визначені стадії несанкціонованої дії:

- прихований етап - дія ШПЗ не виявляється і залишається непоміченою;

- лавиноподібне розмноження, але його дії на цій стадії не активізовані (зазначений етап притаманний не всім ШПЗ);

- активні дії - виконуються шкідливі дії, закладені його розробником.

Також характерною рисою всіх ШПЗ є їх активізація, що пов'язана з різними подіями, а саме:

- настанням певної події, дати або дня тижня;

- запуском програмного засобу;

- відкриттям документа і т.п.

Підводячи підсумок цього дослідження необхідно зазначити, що криміналістична класифікація ШПЗ має ряд визначених особливостей, що відрізняє їх від інших суспільно небезпечних явищ. По-перше, використання ШПЗ не вимагає фізичного зближення ЕОТ потерпілої особи з правопорушником в момент вчинення злочину. По-друге, злочини пов’язані з ШПЗ є технічно автоматизованими. Тобто, за короткий термін часу правопорушник може збільшити кількість вчинених злочинів та потерпілих осіб в декілька разів. По-третє, на використання ШПЗ не можна поширити обмеження, превентивні заходи, що є в реальному, фізичному світі. Так, несанкціоноване втручання в ЕОТ за допомогою ШПЗ може вчинятися в досить короткий термін часу та потребує швидкої реакції захисту у відповідь. По-четверте, злочини, що вчиняються за допомогою ШПЗ і до цього часу залишаються новим явищем в злочинній сфері і тому криміналістична класифікація ШПЗ надасть змогу своєчасно оцінити загрози кібербезпеці, вжити адекватних заходів реагування та ефективно здійснювати документування протиправної діяльності, а також встановлення осіб, що їх вчинили.

Існуюча класифікація ШПЗ на даний час має розрізнений характер та характеризує ШПЗ лише за певними їх особливостями. Тому, при криміналістичній класифікації необхідно враховувати, що ШПЗ одночасно може володіти декількома своїми властивостями з різних їх видів. У зв'язку з такою ситуацією виникла необхідність у створенні універсальної криміналістичної кваліфікації (класифікатора) ШПЗ яка б охоплювала опис ШПЗ та надавала б змогу здійснювати їх опис з урахуванням різних їх характеристик, а саме: середовищем існуванням, зовнішнім виглядом, результатом деструктивної діяльності, способом ураження, алгоритмом дії.

В багатьох випадках завдяки такій узагальненій класифікації буде вирішено наступні задачі. По-перше, об'єднуються вже існуючі класифікації ШПЗ. По-друге, опис такого ШПЗ буде мати уніфікований та універсальний характер, що дасть можливість більш об'єктивно провести характеристику того чи іншого ШПЗ та більш точно віднести його до конкретно визначеного виду.

Література:

1. Біленчук П. Д. Комп'ютерна злочинність. [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.] Навчальний посібник. К: "Атіка", 2002. – 240 с.

2. Савченко О. В. Документування несанкціонованого втручання в роботу автоматизованих систем та мереж електрозв'язку, що призвело до блокування інформації (DDOS-атаки) / Відп.ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009 р.: тези допов. – К., 2009. – 114 с. (С. 77–82).

3. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навчальний посібник, – К.: Атіка, 2002. – 240 с.

4. Гавловський В. Д., Тітуніна К. В. Актуальні питання міжнародного співробітництва у боротьбі з комп'ютерною злочинністю. / Відп. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: міжвідомчий семінар-нарада, 28–29 травня 2009р.: тези допов. – К., 2009. – 114 с. (С. 36–42).

5. Звіт Cisco від Intecracy Group: Midyear Cybersecurity Report. [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/dam/m/digital/elq-

cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2

6. Державні статистичні відомості. [Електронний ресурс] / Офіційний веб-сайт Генеральної прокуратури України. — Режим доступу : (https://www.gp.gov.ua/ua/stst2011.html?dir_id=113277&libid=100820&c=edit&_c=fo)

7. Протасевич А. А. Борьба с киберпреступностью как актуальная задача современной науки / А. А. Протасевич, Л.П. Зверянская // Криминологический журнал ГУЭП. – 2011. – № 3. – С. 28–33.

8. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук : спец. 12.00.08 / Алексей Васильевич Суслопаров. – Красноярск, 2010. – 206 с.

9. www.caro.org

10. https://cme.mitre.org

References:

1. Bilenchuk P. D. Komp'juterna zlochinnist'. [P. D. Bilenchuk, B. V. Romanjuk, V. S. Cimbaljuk ta in.] Navchal'nij posibnik. K: "Atika", 2002. – 240 s.

2. Savchenko O. V. Dokumentuvannja nesankcionovanogo vtruchannja v robotu avtomatizovanih sistem ta merezh elektrozv'jazku, shho prizvelo do blokuvannja informacii (DDOS-ataki) / Vidp.red. L. P. Skalozub, V. I. Vasilinchuk, S.A.Lebid' // Organizacija protidii zlochinam u sferi intelektual'noï vlasnosti ta komp'juternih tehnologij: mizhvidomchij seminar-narada, 28–29 travnja 2009 r.: tezi dopov. – K., 2009. – 114 s. (S. 77–82).

3. Bilenchuk P. D., Romanjuk B. V., Cimbaljuk V. S. ta in. Komp'juterna zlochinnist'. Navchal'nij posibnik, – K.: Atika, 2002. – 240 s.

4. Gavlovs'kij V. D., Titunina K. V. Aktual'ni pitannja mizhnarodnogo spivrobitnictva u borot'bi z komp'juternoju zlochinnistju. / Vidp. red. L. P. Skalozub, V. I. Vasilinchuk, S. A. Lebid' // Organizacija protidiï zlochinam u sferi intelektual'noï vlasnosti ta komp'juternih tehnologij: mizhvidomchij seminar-narada, 28–29 travnja 2009r.: tezi dopov. – K., 2009. – 114 s. (S. 36–42).

5. Zvit Cisco vid Intecracy Group: Midyear Cybersecurity Report. [JElektronnyj resurs]. — Rezhim dostupa: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2

6. Derzhavni statistichni vidomosti. [Elektronnij resurs] / Oficijnij veb-sajt General'noï prokuraturi Ukraïni. — Rezhim dostupu : (https://www.gp.gov.ua/ua/stst2011.html?dir_id=113277&libid=100820&c=edit&_c=fo)

7. Protasevich A. A. Bor'ba s kiberprestupnost'ju kak aktual'naja zadacha sovremennoj nauki / A.A. Protasevich, L.P. Zverjanskaja // Kriminologicheskij zhurnal GUJEP. – 2011. – № 3. – S. 28–33.

8. Susloparov A. V. Komp'juternye prestuplenija kak raznovidnost' prestuplenij informacionnogo haraktera : dis. ... kand. jurid. nauk : spec. 12.00.08 / Aleksej Vasil'evich Susloparov. – Krasnojarsk, 2010. – 206 s.

9. www.caro.org

10. https://cme.mitre.org